PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-308733
(43)Date of publication of application : 17.11.1998

(51)Int.Cl. H04L 9/32
G09C 1/00
// G06F 13/00

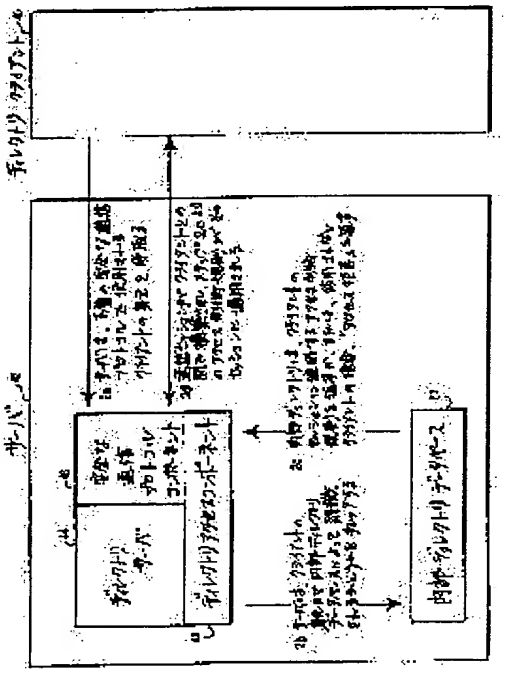
(21)Application number : 10-047343
(22)Date of filing : 27.02.1998

(71)Applicant : XCERT SOFTWARE INC
(72)Inventor : RICHARD PATRICK
CSINGER ANDREW
KNIPE BRUCE
WOODWARD BRUCE

(30)Priority
Priority number : 97 808846 Priority date : 28.02.1997 Priority country : US

(54) METHOD FOR PROVIDING SECURE COMMUNICATION, AND DEVICE FOR PROVIDING SECURE DIRECTORY SERVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a secure public key infrastructure.
SOLUTION: A server 42 receives an identification name(DN) of a client 40 and searches a directory for identification information and an access control right. The client 40 receives a DN of the server 42, uses directory service and decides the server's 42 identity. Identity decision is performed based on specifying the directory service. Some directory service issues identities (DN) of the server 42 and the client 40, and the 'home' directory service is specified. Directory services mutually communicate and mutually offer a list of electronic identities. With this, the client 40 or the server 42 verifies the identity of a communicator based on a trusted 'home' directory service. Public key certificates, a certificate cancel list, an undecided certificate request and a certificate authority policy or the other are stored in a directory server.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－308733

(43)公開日　平成10年(1998)11月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｅ
// Ｇ０６Ｆ　13/00	３５７	Ｇ０６Ｆ　13/00	３５７Ｚ

審査請求　未請求　請求項の数53　ＯＬ　（全 19 頁）

(21)出願番号　特願平10－47343

(22)出願日　平成10年(1998)２月27日

(31)優先権主張番号　０８／８０８８４６

(32)優先日　1997年２月28日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　598027032
エクサート・ソフトウェア・インコーポレイテッド
XCERT SOFTWARE INC.
カナダ、ブイ・７・ワイ　１・シィ・６　ブリティッシュ・コロンビア州、バンクーバー、パシフィック・センタ、ピィ・オゥ・ボックス・10145、ダブリュ・ジョージア・ストリート、701、スウィート・1001

(74)代理人　弁理士　深見　久郎　（外３名）

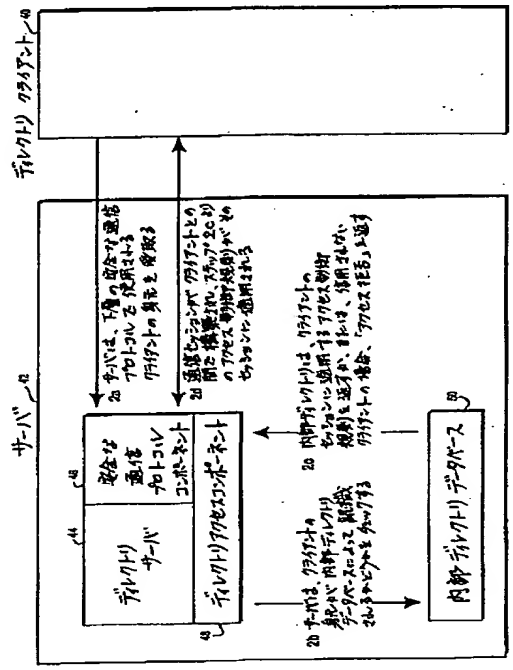
最終頁に続く

(54)【発明の名称】　安全な通信を提供するための方法、および安全なディレクトリサービスを提供するための装置

(57)【要約】

【課題】　安全な公開鍵インフラストラクチャを提供する。

【解決手段】　サーバはクライアントの識別名（ＤＮ）を受取り、識別情報およびアクセス制御権に関しディレクトリをサーチする。クライアントはサーバのＤＮを受取り、ディレクトリサービスを使用してサーバの身元を判定する。身元の判定は、ディレクトリサービスを特定できることに基づく。サーバおよびクライアントは、何らかのディレクトリサービスから身元（ＤＮ）を発行され、その「ホーム」ディレクトリサービスを特定できる。ディレクトリサービスは、相互に通信して、電子的身元のリストを提供し合う。これにより、クライアントまたはサーバは、信頼された「ホーム」ディレクトリサービスに基づいて、通信者の身元を検証できる。ディレクトリサーバ内には、公開鍵証明書、証明書取消しリスト、未決証明書要求、証明権威ポリシーその他が記憶される。



1

【特許請求の範囲】

【請求項１】　第１のワークステーションにおけるクライアントとコンピュータとの間に安全な通信を提供するための方法であって、

前記コンピュータにおいて、情報およびサービスの少なくとも１つに対するリクエストを前記クライアントから受取るステップを含み、前記リクエストは前記クライアントを特定する少なくとも１つのデジタル証明書を含み、さらに、

前記コンピュータにおいて、前記デジタル証明書の発行者が認識されるかどうかを判定するためにチェックを行なうステップと、

前記デジタル証明書が有効であるかどうかを検証するステップと、

デジタル証明書が有効であれば、情報およびサービスの少なくとも１つが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべきアクセス制御規則を検索するステップとを含む、方法。

【請求項２】　前記アクセス制御規則を通信セッションに適用するステップをさらに含む、請求項１に記載の方法。

【請求項３】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項１に記載の方法。

【請求項４】　前記受取るステップは、クライアントの公開鍵を受取るステップを含む、請求項１に記載の方法。

【請求項５】　前記コンピュータは内部データベースを含み、前記チェックを行なうステップは、特定された証明する側の関係者の公開鍵が前記内部データベース内に記憶されているかどうかを判定するためにチェックを行なうステップを含む、請求項１に記載の方法。

【請求項６】　前記コンピュータはディレクトリを含み、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ディレクトリにアクセスできるようにするステップを含む、請求項２に記載の方法。

【請求項７】　前記クライアントは前記リクエストを介してウェブサイトへのアクセスを要求し、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ウェブサイトにおいて動作することができるようにするステップを含む、請求項２に記載の方法。

【請求項８】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項５に記載の方法。

【請求項９】　第１のワークステーションにおけるクライアントとコンピュータとの間で安全な通信を提供するための方法であって、

前記コンピュータにおいて、情報およびサービスのうち

2

少なくとも１つに対する前記クライアントからのリクエストを受取るステップを含み、前記リクエストは前記クライアントを一意に特定し、さらに、

前記コンピュータにおいて、クライアントが前記コンピュータによって認識されるかどうかを判定するためにチェックを行なうステップと、

クライアントが認識されれば、情報およびサービスの少なくとも１つが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべきアクセス制御規則を検索するステップと、

前記アクセス制御規則を前記クライアントとの通信セッションに適用するステップとを含む、方法。

【請求項１０】　前記受取るステップはデジタル証明書を通じてクライアントを一意に特定するステップを含む、請求項９に記載の方法。

【請求項１１】　前記受取るステップは、クライアントの公開鍵を含んでクライアントを一意に特定するデータを受取るステップを含む、請求項９に記載の方法。

【請求項１２】　前記コンピュータは内部データベースを含み、前記チェックを行なうステップは、特定された証明する側の関係者の公開鍵が前記内部データベース内に記憶されているかどうかを判定するためにチェックを行なうステップを含む、請求項１０に記載の方法。

【請求項１３】　前記コンピュータはディレクトリを含み、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ディレクトリにアクセスできるようにするステップを含む、請求項９に記載の方法。

【請求項１４】　前記クライアントは前記リクエストを通じてウェブサイトへのアクセスを要求し、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ウェブサイトにおいて動作することができるようにするステップを含む、請求項９に記載の方法。

【請求項１５】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項９に記載の方法。

【請求項１６】　第１のワークステーションにおけるクライアントとコンピュータとの間に安全な通信を提供するための方法であって、

前記コンピュータにおいて、情報およびサービスのうち少なくとも１つに対する前記クライアントからのリクエストを受取るステップを含み、前記リクエストは前記クライアントを特定する少なくとも１つのデジタル証明書を含み、さらに、

前記コンピュータにおいて、前記デジタル証明書内のデジタル署名が有効であるかどうかを判定するためにチェックを行なうステップと、

情報およびサービスのうち少なくとも１つが前記クライアントに提供される、前記クライアントとの通信セッシ

ョンに適用すべきアクセス制御規則を検索するステップとを含む、方法。

【請求項１７】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項１６に記載の方法。

【請求項１８】　前記制御規則をクライアントとの通信セッションに適用するステップをさらに含む、請求項１６に記載の方法。

【請求項１９】　前記コンピュータは内部データベースを含み、前記チェックを行なうステップは、特定された証明される側の関係者の公開鍵が前記内部データベース内に記憶されているかどうかを判定するためにチェックを行なうステップを含む、請求項１６に記載の方法。

【請求項２０】　前記コンピュータはディレクトリを含み、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ディレクトリにアクセスすることができるようにするステップを含む、請求項１８に記載の方法。

【請求項２１】　前記クライアントは前記リクエストを介してウェブサイトへのアクセスを要求し、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ウェブサイトにおいて動作を行なうことができるようにするステップを含む、請求項１８に記載の方法。

【請求項２２】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項１６に記載の方法。

【請求項２３】　複数のコンピュータを含むネットワークに結合された第１のワークステーションにおけるクライアントに安全な通信を提供するための方法であって、
第１のコンピュータにおいて、前記クライアントからの情報およびサービスのうち少なくとも１つに対するリクエストを受取るステップを含み、前記リクエストは前記クライアントを一意に特定し、さらに前記第１のコンピュータにおいて、クライアントが認識されるかどうかを判定するためにチェックを行なうステップと、
前記ネットワークに結合された第２のコンピュータにおいて、クライアントが認識されるかどうかを判定するためにチェックを行なうステップと、
クライアントが認識されれば、情報およびサービスのうち少なくとも１つが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべきアクセス制御規則を前記第２のコンピュータから検索するステップとを含む、方法。

【請求項２４】　前記アクセス制御規則を前記クライアントとの通信セッションに適用するステップをさらに含む、請求項２３に記載の方法。

【請求項２５】　前記クライアントの身元を検証することのできるサーバとして動作するための第２のコンピュータを特定し、かつ、前記第２のコンピュータをインターネットを介して前記第１のコンピュータに相互接続するステップをさらに含む、請求項２３に記載の方法。

【請求項２６】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項２３に記載の方法。

【請求項２７】　前記受取るステップは、デジタル証明書を通じてクライアントを一意に特定するステップを含む、請求項２３に記載の方法。

【請求項２８】　前記受取るステップは、クライアントの公開鍵を含んでクライアントを一意に特定するデータを受取るステップを含む、請求項２３に記載の方法。

【請求項２９】　前記第１のコンピュータおよび前記第２のコンピュータは内部データベースを含み、前記チェックを行なうステップは、特定された証明する側の関係者の公開鍵が前記内部データベース内に記憶されているかどうかを判定するためにチェックを行なうステップを含む、請求項２３に記載の方法。

【請求項３０】　前記コンピュータはディレクトリを含み、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ディレクトリにアクセスできるようにするステップを含む、請求項２４に記載の方法。

【請求項３１】　前記クライアントは前記リクエストを通じてウェブサイトへのアクセスを要求し、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ウェブサイトにおいて動作を行なうことができるようにするステップを含む、請求項２４に記載の方法。

【請求項３２】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項２７に記載の方法。

【請求項３３】　第１のワークステーションにおけるクライアントとコンピュータとの間に安全なディレクトリサービス通信を提供するための方法であって、
情報およびサービスのうち少なくとも１つを得るために、クライアントのワークステーションから前記コンピュータにディレクトリサービスに対するリクエストを送信するステップを含み、前記リクエストは、前記クライアントが後に確実に検証され得る既知の身元を有することを一意に立証するためのデジタル情報を含み、さらに、
クライアントが前記コンピュータによって認識されるかどうかを判定するためにチェックを行なうステップと、
ディレクトリサービスが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべきアクセス制御規則を検索するステップと、
前記アクセス制御規則を前記クライアントとの通信セッションに適用するステップとを含む、方法。

【請求項３４】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含

む、請求項３３に記載の方法。

【請求項３５】　複数のコンピュータを含むネットワークに結合された第１のワークステーションにおけるクライアントに安全な通信を提供するための方法であって、前記複数のコンピュータの各々はディレクトリサーバおよび関連するデータベースを含み、前記方法は、

前記第１のワークステーションから前記複数のコンピュータのうちの第１のコンピュータに、情報およびサービスのうち少なくとも１つに対する前記ユーザからのリクエストを送信するステップを含み、前記リクエストは前記クライアントを一意に特定し、さらに、

クライアントが前記第１のコンピュータによって認識されるかどうかを判定するために、第１のコンピュータのディレクトリサーバによって前記第１のコンピュータにおける関連するデータベースをチェックするステップと、

クライアントが認識されるかどうかを判定するために、前記ネットワークに結合された第２のコンピュータのディレクトリサーバによって前記第２のコンピュータにおける関連するデータベースをチェックするステップと、

クライアントが認識されれば、情報およびサービスのうち少なくとも１つが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべきアクセス制御規則を前記第２のコンピュータから検索するステップとを含む、方法。

【請求項３６】　前記第２のコンピュータの内部データベースからの信頼に関する情報にアクセスするステップをさらに含む、請求項３５に記載の方法。

【請求項３７】　クライアントのリクエストに対して信頼に関する情報およびアクセス制御規則を適用して、許可レベルを越えないことを確実にするためのステップをさらに含む、請求項３６に記載の方法。

【請求項３８】　前記リクエストはウェブサイトに送信される電子商取引に関するリクエストである、請求項３５に記載の方法。

【請求項３９】　リクエストは商取引のためのリクエストであって、クライアントを認識するサーバは関係者のコンテキスト内で取引パラメータを作成する、請求項３５に記載の方法。

【請求項４０】　前記送信するステップは、デジタル証明書を通じてクライアントを一意に特定するステップを含む、請求項３５に記載の方法。

【請求項４１】　前記送信するステップは、クライアントの公開鍵を含んでクライアントを一意に特定するデータを送信するステップを含む、請求項３５に記載の方法。

【請求項４２】　前記第１のコンピュータのディレクトリサーバによってチェックを行なう前記ステップは、特定された証明する側の関係者の公開鍵が前記関連する内部データベース内に記憶されているかどうかを判定するためにチェックを行なうステップを含む、請求項３５に記載の方法。

【請求項４３】　前記アクセス制御規則を適用して、前記アクセス制御規則に従ってのみクライアントが前記ディレクトリにアクセスできるようにするステップをさらに含む、請求項３５に記載の方法。

【請求項４４】　前記クライアントは前記リクエストを通じてウェブサイトへのアクセスを要求し、前記方法はさらに、前記アクセス制御規則を適用して、前記アクセス制御規則に従ってのみクライアントが前記ウェブサイトにおいて動作を行なうことができるようにするステップをさらに含む、請求項３５に記載の方法。

【請求項４５】　第１のワークステーションにおけるクライアントとディレクトリサーバを有するコンピュータとの間に安全なディレクトリサービス通信を提供するための方法であって、

クライアントのワークステーションから前記コンピュータにディレクトリサービスに対するリクエストを送信するステップを含み、前記クライアントからの前記リクエストは情報およびサービスのうち少なくとも１つを含み、前記リクエストは、前記クライアントが後に確実に検証され得る既知の身元を有することを一意に立証するためのデジタル証明書を含み、さらに、

前記ディレクトリサーバによって、サーバが少なくとも１つのデジタル証明書およびそのリクエストのコンテキストに関連する情報に基づいてリクエストに従うための許可を検証するステップと、

ディレクトリサービスが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべき前記アクセス制御規則を検索するステップとを含む、方法。

【請求項４６】　前記アクセス制御規則を前記クライアントとの通信セッションに適用するステップをさらに含む、請求項４５に記載の方法。

【請求項４７】　前記リクエストはクライアントの公開鍵を含む、請求項４５に記載の方法。

【請求項４８】　前記コンピュータは内部データベースを含み、前記検証するステップは、特定された証明する側の関係者の公開鍵が前記内部データベース内に記憶されているかどうかを判定するためにチェックを行なうステップを含む、請求項４５に記載の方法。

【請求項４９】　前記コンピュータはディレクトリを含み、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ディレクトリにアクセスできるようにするステップを含む、請求項４６に記載の方法。

【請求項５０】　前記クライアントは前記リクエストを通じてウェブサイトに対するアクセスを要求し、前記アクセス制御規則を適用する前記ステップは、前記アクセス制御規則に従ってのみクライアントが前記ウェブサイ

トにおいて動作を行なうことができるようにするステップを含む、請求項４６に記載の方法。

【請求項５１】　前記クライアントに関連し得る、信頼の度合に関する情報にアクセスするステップをさらに含む、請求項４５に記載の方法。

【請求項５２】　第１のワークステーションにおけるクライアントによる情報またはサービスに対するリクエストに応答しながら安全なディレクトリサービスを提供するための装置であって、

前記クライアントのワークステーションから情報およびサービスのうち少なくとも１つを含むディレクトリサービスに対するリクエストを受取るための安全な通信入力モジュールを含み、前記リクエストは、前記クライアントが後に確実に検証され得る既知の身元を有することを一意に立証するためのデジタル証明書を含み、さらに、前記リクエストに応答するためのディレクトリサーバモジュールと、

クライアントのデジタル証明書の発行者の公開鍵を示す情報を記憶しかつリクエストに適用するアクセス制御規則を記憶するためのデータベースとを含み、

前記ディレクトリサーバモジュールは、サーバがリクエストに、少なくとも１つのデジタル証明書およびそのリクエストのコンテキストに関連する情報に基づいて従うことに関する許可を検証するよう動作可能であり、かつ、ディレクトリサービスが前記クライアントに提供される、前記クライアントとの通信セッションに適用すべきアクセス制御規則を検索するためのものである装置。

【請求項５３】　前記ディレクトリサーバモジュールは、前記アクセス制御規則を前記クライアントとの通信セッションに適用するよう動作可能である、請求項５２に記載の装置。

【発明の詳細な説明】

【０００１】

【発明の分野】この発明は一般に、ワークステーションでのユーザがサーバコンピュータから情報またはサービスを要求する、デジタルデータ処理通信システムの分野に関する。より特定的にはこの発明は、コンピュータシステムおよび／またはコンピュータネットワーク内に、安全なディレクトリサービスによって公開鍵インフラストラクチャを提供するための方法および装置に関する。

【０００２】

【発明の背景および概要】ネットワークを用いた通信が広く使用されさらに急成長を遂げる中、ビジネス界の多くの人々は長年、電子処理による商取引が当たり前となるような状況を思い描いてきた。電子商取引を広げる上での大きな障害となっているのは、プライバシー、メッセージの完全性、認証力を提供しかつ拒絶の生じない、安全な通信システムを有効に展開しなくてならないことである。

【０００３】多種多様のネットワーク上で通信されるメッセージのプライバシーおよび認証力を保証するために、暗号方式が広く使用されてきている。従来技術による暗号方式の多くは、たとえばキー配送等に関する広く認識されている問題を抱えるため、商取引の世界で広く展開するのには不十分である。

【０００４】キー配送の問題を含む既存の暗号方式上の問題を解決するために、公開鍵暗号方式が有利に利用されてきている。これら公開鍵暗号方式は、公開鍵と秘密鍵との対を使用して暗号化のプロセスと復号のプロセスを分離しており、それにより、暗号化プロセスの鍵と復号化プロセスの鍵とが全く別であるようにしている。このようなシステムでは、暗号化の鍵がわかっていてかつ十分大きい暗号化鍵が与えられたとしても、復号鍵を算出することができないため、ユーザの暗号化鍵を配送または公開することができる。ある特定の宛先のユーザとの通信を希望する際には、その宛先ユーザの公開鍵の下でメッセージを暗号化する。送信されたメッセージは、その公開鍵／秘密鍵の対の、秘密の復号鍵を持つ宛先ユーザのみが暗号解読できるのである。

【０００５】公開鍵暗号方式においては、信頼された権威が、要請元の公開鍵および要請元の名称を含むデジタルメッセージを作成することが可能であることが知られている。その信頼された権威の代表者は、その権威自身のデジタル署名で、そのデジタルメッセージに電子的に署名する。このようなデジタルメッセージはデジタル証明書と称され、使用される要請元自身のデジタル署名とともに送信される。実用的な公開鍵暗号方式の実現のための例示的方法を開示する、リベスト（Rivest）等に発行された米国特許番号第４，４０５，８２９号を参照されたい。デジタル署名の証明が改善された、公開鍵デジタル署名暗号方式を開示する米国特許番号第５，２１４，７０２号もまた参照されたい。

【０００６】既存の公開鍵暗号方式は、電子商取引に地球規模の規格を使用して、Ｘ．５００規格と称される規格で公開鍵の使用をハイレベルの地球規模の権威と結び付けることを想定している。しかし、すべてのユーザがこの地球規模の規格に参入しているわけではないので、規格の実用性には限界がある。

【０００７】本発明による方法は、地球規模の規格に依存しない。この発明の例示的な実施例に従えば、暗号鍵は、ユーザ自身のディレクトリサービス内に常駐することが可能であり、かつここに開示する分散ディレクトリサービスを使用することによってユーザが互いに安全に通信できるようにできる。この発明は、安全な分散ディレクトリサービスを利用して、公開鍵インフラストラクチャを維持する。所望のレベルのセキュリティを提供するためにすべてのユーザを証明しなくてはならない「超証明者」を使用する、従来技術による地球規模のトップダウン式の階層構造で動作するものではない。

【０００８】例示的な実施例に従えば、ユーザは他のさ

まざまなユーザからデジタル証明書を受取りながら十分なセキュリティを保って互いに安全に通信することができ、電子商取引を実現することができる。この発明は、ポリシーステートメントを使用するが、ポリシーステートメントは、メッセージの受取人がメッセージの送り手の身元を分散ディレクトリサービスシステムを通じて分析し、それに基づいて、ユーザのサービス要求に対して効率的に信用レベルを適用することを可能にする。したがって、あるメッセージの送り手が指定されたポリシーステートメントを使用して所与の分散ディレクトリサービス内で識別されれば、メッセージの受取人はメッセージの送り手に与えるべき信用の度合いを判定することができるのである。

【０００９】この例示的実施例は、特定の通信コンテキスト内でクライアントを一意に識別することができることによって、サーバがそのコンテキストに関して特定のアクセス権をクライアントに割当てることが可能となる、という概念を実現する。クライアントに許可されるアクセス権は、そのコンテキストにおけるそのクライアントの身元に依存する。

【００１０】アクセス権が身元に応じて与えられるわけであるから、クライアントを一意に識別できるという特徴は重要性を帯びてくる。サーバには、クライアントを識別する安全かつ確実な方法が必要となる。この確実な方法は、この発明の例示的な実施例に記載した性質を有する、安全なディレクトリサービスを使用するものである。ディレクトリサービスから身元検証サービスを安全に受取ることによって、サーバはクライアントに許可すべきアクセス権を判定することができる。これによって、サーバはクライアントに関する知識を事前に有さずとも、クライアントに依存する情報を提供することが可能となる。

【００１１】この発明の例示的実施例に従えば、クライアントはまず、ディレクトリサービスを提供するサーバとの安全な接続を開始する。サーバは、ここに開示する安全な通信方法における認証という特徴を利用して、クライアントを一意に識別してそのクライアントの識別名（ＤＮ）を獲得する。サーバはこのクライアントのＤＮを使用して、クライアントにどのようなアクセス権を許可するかを判定するが、これは、自身のディレクトリ内にあるクライアントのＤＮをルックアップするか、または、その特定のＤＮについての確実な情報を含む別のディレクトリサーバに対してクライアントとして再帰的に動作するか、のいずれかによって判定される。その後、ディレクトリサーバがそのクライアントに特有の情報をクライアントに返すが、これは、ここで使用する安全な通信方法によって提供される認証という特徴を利用することによって可能となる。

【００１２】この発明の別の局面に従えば、クライアントはサーバとの安全な通信を開始する。ここに記載する方法はまた、クライアントとサーバが同じ機械内に存在する場合にも適用が可能であり、したがって、ここで説明するネットワークが、この場合にはコンピュータの内部であり得る。サーバは、ディレクトリサービスとしての安全な通信サーバの認証という特徴に基づいて、クライアントを一意に識別して、クライアントのＤＮの身元を検証し、また、クライアントにアクセス制御許可を与えることができる。ディレクトリサービスとのこの通信は、安全な通信チャネル上で行なわれなくてはならない。なぜなら、クライアント／サーバ間の通信でやり取りされる情報が、ディレクトリサービスから返された結果、検証およびアクセス権に依存するためである。ディレクトリサービスは、サーバに応答して、そのクライアントに特定の検証情報およびアクセス制御情報を返し、サーバは、どの情報をクライアントに送るべきかを判定することができる。サーバはその後、クライアントによって要求された情報のうちすべてまたは一部を返すか、全く情報を返さないかのいずれかである。

【００１３】例示的な実施例においては、関係者の身元が、ディレクトリサービスの通信コンテキストに関するアクセス権を決定する。クライアントによってなされたすべての情報要求は、カスタマイズされたディレクトリサービス応答を受取る。ピアの身元は、安全な通信を使用することによって判定される。

【００１４】例示的な実施例においては、サーバはクライアントの識別名（ＤＮ）を受取って、その後、その特定のコンテキストに関する識別情報およびアクセス制御権を求め、そのディレクトリをサーチする。サーバは、スタンドアローンサーバとして、または、ネットワーク上の他のディレクトリサービスと関連して動作することが可能である。クライアントは、安全な通信を続けるために検証可能な身元を有さねばならない。クライアントの身元は、もしサーバがそのクライアントのＤＮを保持するディレクトリサービスにアクセスできれば、十分に検証可能であるということができる。

【００１５】クライアントはサーバのＤＮを受取り、その後、クライアントは情報要求に対する応答を受入れるかどうか（すなわち、応答を信用するかどうか）を判定することができる。クライアントは、何らかのディレクトリサービスを使用してサーバの身元を判定する（クライアントは、スタンドアローンまたは、他のディレクトリサーバのクライアントとして動作することができる）。サーバは、もしクライアントがサーバのＤＮを保持するディレクトリサービスを特定することができれば、十分に検証可能であるといえる。

【００１６】いずれの場合にも、身元の判定は、ディレクトリサービスを識別することができるという事実に基づく。サーバおよびクライアントは、それらが安全な通信に参加する前に何らかのディレクトリサービスから身元（ＤＮ）を発行されるので、それらは少なくとも自身

の「ホーム」ディレクトリサービスを特定することができる。それらの「ホーム」ディレクトリサービスは他のディレクトリサービスと通信し、各々が、安全なディレクトリサービスを使用して互いに対して電子的身元のリストを「提供する」。このようにして、クライアントまたはサーバは、信用できる「ホーム」ディレクトリサービスに基づいて、安全な通信者のピアの身元を検証することができる。

【００１７】本発明のこの例示的な実施例は、以下の方法で公開鍵インフラストラクチャを実現するのに使用することができる。すなわち、公開鍵証明書、証明書取消しリスト、未決証明書要求、証明権威ポリシー、その他の情報がディレクトリサーバ内に記憶される。ディレクトリサーバへのアクセスは、安全な通信を介して行なわれる。これにより、情報の完全性およびプライバシーが維持される。証明権威の資格で活動する管理者は、「管理者用ＤＮ」を発行されることによって、リポジトリへのフルアクセスを許可され、新しい証明書を付加することも、証明書取消しリストを修正することもできる。他の者に許可されるアクセスはこれより少なく、知られていない関係者に至っては、証明書要求を提出するか、または、公開証明書（および取消しリスト）をダウンロードすることのみしか許可されないであろう。また、証明書はディレクトリサーチのベクトルとして使用することができる。すなわち、ディレクトリサーチを試みるクライアントは、そのクライアントのＤＮによってアクセスが制限される。クライアントのＤＮは名称を全く含まず、代わりにクライアントのポリシーのハッシュを含み得る。この方法によって、最小限の情報を含む証明書を発行することが可能となる。実際に、証明書は、ベクトル空間（これは、その特定のクライアントが見ることのできる全体の名称空間である）内でベクトルとして使用することのできる一意の識別子を含んでいさえすればよい。

【００１８】この発明のこれらおよび他の特徴は、添付の図面に関連して以下のこの発明の好ましい実施例の説明を読むことにより、より良く理解されるであろう。

【００１９】

【この発明の例示された実施例の詳細な説明】図１は、この発明がその中で電子商業／通信ネットワークの一部として利用され得る、例示的な計算システムをブロック図で示す。この発明に従った方法はこのような通信ネットワーク環境において利用できる他に、データのセキュリティが重要な関心事であって実際に実現可能であるような、１以上のラップトップコンピュータ、スタンドアローン、ＰＣ型コンピュータ、ミニコンピュータ、および他のいかなるコンピュータシステム環境をも含む、広範囲のデータ処理システムと関連して使用することも可能である。

【００２０】この発明に関連して使用され得る例示的な通信システムを説明する前に、ここで利用する用語についてまず説明する。「クライアントプロセス」またはプログラムは、ネットワークに接続されたコンピュータ上で実行される。クライアントプロセスは、情報またはサービスを要求するという特徴を有する。クライアントプロセスは、ここではクライアントと称される。

【００２１】「サーバプロセス」もまた、ネットワークに接続されたコンピュータ上で実行される。サーバプロセスは、情報またはサービスに対する要求を満たすという特徴を有する。サーバプロセスは、ここではサーバと称される。なお、クライアントおよびサーバは、実際には同じコンピュータ上で実行される場合があり、また、サーバは、別のサーバに対するクライアントでもあり得る。

【００２２】ここで使用される場合、「安全な通信」とは典型的に、好ましくは、プライバシー、メッセージの完全性、および認証性を提供しかつ拒絶されることのない、データ転送機構を意味するが、それらに限定されるものではない。

【００２３】「識別名」（ＤＮ）は、好ましくは安全な通信を通じて可能となるデジタル会話に参加するエンティティを一意に識別する。

【００２４】「通信コンテキスト」とは、クライアントが何らかのサーバからの情報を要求し、その情報への要求が、クライアントのＤＮ、サーバのＤＮ、要求される情報、入手可能な情報、およびその情報に対するアクセス制御のうちの１以上の項目によって特徴付けられ得る、状況を意味する。

【００２５】再び図１を参照して、この図は、ローカルネットワークを介して、およびインターネットを通じて相互接続される多数のクライアント計算装置、および、クライアント／サーバ計算サービスの組合せを含む、例示的な通信ネットワークを示す。図１に示されるローカルエリアネットワーク（ＬＡＮ）、すなわちＬＡＮ１およびＬＡＮ１３は、例示の目的のみで図示されたものである。これらのネットワークは、クライアントおよびサーバが接続されたイーサネット（登録商標）、トークンリング、または、他の種類のネットワーク等の、図１のアーキテクチャに同様に包含され得る多くのネットワーク設計のうちいずれかを代表するものであると理解されたい。例示の目的のみで、ＬＡＮ１はイーサネット８０２．３　１０ベースＴネットワークであり得る。種々のプロトコルがＬＡＮ１上で実行されるが、これは、ＴＣＰ／ＩＰおよびＮＥＴＢＩＯＳ等を含む。数多くのプロトコルがＬＡＮ１上で実行可能であるが、インターネット上で実行される、ＴＣＰ／ＩＰの利用が好ましい。

【００２６】図１に示すように、ＬＡＮ１はクライアントとしてのみ動作するＰＣ型コンピュータ２を含む。これはたとえば、Ｗｉｎｄｏｗｓ９５（登録商標）を使用したワークステーションである。この他にもＬＡＮ１は

ワークステーション３を含む。これはたとえば、クライアントおよびサーバの両方として動作する、ＩＢＭ（登録商標）　ＲＳ６０００である。ＩＢＭ　ＲＳ６０００は典型的に、ＡＩＸオペレーティングシステムを実行する。クライアント／サーバ３は、ここに記載した方法論のコンテキスト内ではクライアントとして実行され、および／または、それ自身がＸ．５００ディレクトリ空間を有するサーバとして実行され得る。

【００２７】ＬＡＮ１はまた、ミニコンピュータサーバ４を含む。これは市販のミニコンピュータのいずれでもあり得る。ミニコンピュータサーバ４は、たとえば、デジタル証明書またはディレクトリサービスを提供するのにもっぱら使用される。ミニコンピュータサーバ４は、別のネットワーク（図示せず）に接続されていてもよい。ミニコンピュータサーバ４が含まれていることからもわかるように、サーバはワークステーション型の装置に限定されるものではない。

【００２８】ＬＡＮ１はたとえば、グラフィックスを使用するＳＧＩクライアント／サーバ６もまた含んでもよい。これは、シリコン・グラフィックス（登録商標）・コーポレーション（Ｓｉｌｉｃｏｎ　Ｇｒａｐｈｉｃｓ（登録商標）　Ｃｏｒｐｏｒａｔｉｏｎ）によって製造されるワークステーションのうちの１つであり得る。クライアント／サーバ６は、コンピュータグラフィックスおよび／またはＣＡＤ演算を実行することが可能である。ワークステーションクライアント８はたとえば、ＩＢＭ　ＰＣを使用したワークステーションであって、必要に応じてＬＡＮ１に結合され得る、利用可能な多数の付加的なワークステーションを表わすものである。

【００２９】この発明のディレクトリサービスとの安全な通信は、例示のＬＡＮ１上でのみ行なわれるわけではなく、ＬＡＮ１３上でもまた行なわれる。ＬＡＮ１３もまた、インターネット通信のためのＴＣＰ／ＩＰを含むプロトコルで実行される。

【００３０】ＬＡＮ１および１３は、たとえば、インターネット２２を介して、ルータ１６および１８を介して通信する。ルータ１６および１８は、インターネット通信のための従来技術による経路制御コンピュータであって、必要な経路制御機能を行ないかつインターネット上で関連するデバイスの記録を保持するのに十分なメモリ容量を有する。ルータは、インターネット上で２つの装置をすばやく接続することができる。ルータ１６、１８は、２以上のＬＡＮのために動作する場合もある。ルータ１６および１８はたとえば、シスコ（登録商標）・コーポレーション（Ｃｉｓｃｏ（登録商標）　Ｃｏｒｐｏｒａｔｉｏｎ）によって市販されているルータであってもよい。

【００３１】スマートカードリーダ２０およびラップトップクライアント２４等の、他の種々のクライアントもまた、電話線２３、２５を介してインターネットを通じて、描かれている他の装置のいずれかに接続されまたそれらと通信することが可能である。スマートカードリーダ２０はたとえば、Ｖｉｓａカードリーダであり得る。これまでに記載してきた「クライアント」の概念は、情報またはサービスを要求するプログラムに対して適用されたものであったが、スマートカードリーダ２０に関しては、クライアントとは、たとえば、スマートカードリーダ内に実現される、情報またはサービスを要求するハードウェアまたは回路でもあり得る。

【００３２】ＬＡＮ１３は、クライアント／サーバ１２を含む。これはたとえば、ＲＩＳＣ型ワークステーションである、ＳＵＮマイクロシステムズＳＰＡＲＣであってもよい。ＬＡＮ１３はまた、クライアントワークステーション１０を含む。これは、アップル（登録商標）・コーポレーション（Ａｐｐｌｅ（登録商標）　Ｃｏｒｐｏｒａｔｉｏｎ）によって製造されたＭａｃ（登録商標）　ＩＩであってもよい。ＤＥＣ（登録商標）ワークステーションであり得るクライアント／サーバ１４もまたＬＡＮ１３に含まれる。ワークステーション１０、１２および１４は、ＬＡＮに結合され得るワークステーションを例示するものであって、その各々は、異なるオペレーティングシステムで実行され得る。

【００３３】ＬＡＮ１および１３はインターネット２２を介して互いに結合されているが、この方法および装置は、インターネット接続を使用せずとも有利に利用することが可能である。したがって、たとえば、オフィス内ネットワークが、この発明に従ってデジタル証明書および安全な情報を配送することが可能である。この発明が、図１に示す構造のいかなるサブセットにも用いられ得ることが理解されるであろう。

【００３４】図２は、この発明の例示の実施例に従って、ディレクトリクライアント４０とサーバ４２との間で通信されるデータを例示的に示すデータフロー図である。ディレクトリクライアント４０はたとえば、図１に関連して上に記載した、列挙されたクライアントのいずれであってもよい。同様に、サーバ４２はたとえば、図１で上に説明したサーバのいずれであってもよい。ディレクトリサーバ４４、安全な通信プロトコルコンポーネント４６、ディレクトリアクセスコンポーネント４８、および内部ディレクトリデータベース５０が、サーバ計算装置４２内に常駐する。上に記載したように、ディレクトリクライアント４０は、サーバ４２から情報またはサービスを要求する。クライアント４０は、ディレクトリクライアントとして識別され、したがって、ディレクトリ情報を探している。ディレクトリそのものは、事実上、図１のネットワーク内のどの場所に分散し常駐していてもよい。ディレクトリは、たとえば、個人別電話帳内に含まれ得る、個人ユーザおよび法人に関する情報を格納する。たとえば、ディレクトリは、クライアントの識別名または別の一意のクライアント識別子を含むクラ

イアントデータを含み得る。クライアント識別子に加えて、ディレクトリは、安全に通信を交わしたい関係者の公開鍵を識別するための公開鍵情報を記憶する場合もある。サーバ４２内のディレクトリサーバ４４は、予め構築されたディレクトリプロトコルに従って動作して、ディレクトリ情報をディレクトリクライアントに提供する。もしディレクトリサーバ４２が関連する内部データベース５０にアクセスすることによってクライアントのディレクトリに関するキューリーに満足に応答することができるようであれば、サーバ４２は的確に応答することができる。もしそうでなければ、サーバ４４がその質問に応答して、応答できるサーバの位置を識別する照会をディレクトリクライアント４０に返す。これに代えて、ディレクトリサーバ４４は、他のディレクトリサーバとチェーン接続されてもよく、ディレクトリクライアント４０に照会を送信するのではなく、問合せに対する答えを見つけるよう試みることが可能である。このコンテキストにおいては、ディレクトリサーバ４４は別のディレクトリサーバに対するクライアントとして動作する。

【００３５】安全な通信プロトコルコンポーネント４６は、ディレクトリクライアント４０が安全な通信プロトコルを使用してディレクトリサーバ４４と確実に通信できるようにする。安全な通信プロトコルは好ましくは、クライアント４０とサーバ４２との間の通信に対して、プライバシー、認証性および完全性を提供しかつ拒絶がないようにする。従来技術によるシステムにおいては、クライアントがサーバにアクセスする資格を与えられていない場合には、応答が提供されない。この発明に従えば、クライアント４０が要求された情報を得るのに十分な特権を有しているかどうかを示す応答を、ディレクトリサーバから得ることができる。これについては、下にさらに説明する。

【００３６】サーバ４２のディレクトリアクセスコンポーネント４８は、サーバの内部データベース５０との通信を可能にする。サーバ４２は、ディレクトリアクセスコンポーネント４８を介して、クライアント４０がどの種のアクセスを有する資格を与えられるかを判定する。

【００３７】動作において、ステップ２ａに従って、サーバ４２は下層の安全な通信プロトコルを使用して、ディレクトリクライアント４０からクライアントの身元を受取る。この通信プロトコルが認証性を保証するため、クライアントは安全に識別されて、サーバは、後に検証され得る既知の身元を受取る。

【００３８】図３および図４は、安全な通信プロトコルを使用してクライアントがいかに識別され得るかの一例を示す。図３に例示されるように、クライアント６０はサーバ６２とのネットワーク接続を開くことによって、サーバ６２との通信を開始する。この開始の正確な状況は、ネットワークの性質に依存する。サーバ６２はこの

接続に応答して、クライアント６０が自身を特定するよう要求する。クライアント６０はそこで、この通信セッションのための自身の身元を、デジタル証明書の形でサーバ６２に送る。例示の目的のみで、利用される安全な通信プロトコルは、市販のＳＳＬプロトコルであってもよく、これはこの発明に従えば、ディレクトリサービスに有利に適用されて、安全なディレクトリサービスシステムを提供する。

【００３９】図４は、上に図３に関連して説明した、クライアントを特定するのに使用され得る、デジタル証明書６４の一例である。デジタル証明書は、Ｘ．５０９規格内で推奨されるように構築され得るが、これは絶対条件ではない。証明書は、カスタム設計することが可能であり、必要に応じて、種々の異なるおよび／または付加的なフィールドを含み得る。証明書は、たとえば、ＡＳＮ．１文法で書かれ得る。デジタル証明書６４は、デジタル署名シーケンスである「証明書」フィールドを含む。これは、以下に特定されるデータのハッシュを含む。これがその後、署名している側の関係者の秘密鍵で暗号化される。デジタル署名される情報に含まれるものに、バージョン番号と、証明書を一意に識別するシリアル番号と、ＲＳＡ等の識別されたアルゴリズムに従った署名している側の関係者の署名とがある。署名された証明書情報内には、デジタル証明書に署名した関係者の名称を識別する、証明書発行者の識別情報もまた含まれる。証明書は、どの程度の期間その証明書が有効であるかを特定する有効性フィールドを含む。サブジェクトフィールドは、証明書を保持する関係者の名称を特定し、公開鍵情報フィールドは、サブジェクトの公開鍵を特定する。以上に説明したフィールドを拡張して、図４に、それらの構成素構造をより詳細に示す。図４はしたがって、この発明と関連して使用され得る、デジタル証明書の例示的なデータ構造を示すものである。

【００４０】再び図２を参照して、ステップ２ｂに従って、サーバ４２はクライアントの身元が内部ディレクトリデータベースによって認識されるかどうかをチェックする。したがって、もしディレクトリクライアント４０が図４に示すようなデジタル証明書の形でクライアント身元情報を送信する場合、サーバ４２はそのデジタル証明書をチェックして、その内部データベース５０からの認識を確認する。サーバ４２は最初に、デジタル証明書をチェックして、発行者の署名が署名者の署名と合致するかどうかを確認する。したがって、もし内部ディレクトリデータベース５０がその証明書の署名者に関する情報を有していない場合には、クライアントは識別することはできない。このような状況下では、サーバ４２はクライアントとして動作して、要求された署名者の公開鍵情報を別のサーバから検索することによって、身元確認を完了する。このプロセスの詳細は、図６および後続の図に関連して、下により詳細に説明する。

【００４１】クライアントの身元が一旦検証されると、内部ディレクトリは、クライアントの通信セッションに適用するアクセス制御規則を返す。これに代えて、信用されないクライアントの場合には、アクセス拒否が返される場合もある。クライアントの身元が確認されると、アクセス制御リストにアクセスがなされて、その通信セッションに適用されるアクセス規則が検索される。この情報は、ディレクトリアクセスコンポーネント４８を介してディレクトリサービスプロトコル４６に返される。

【００４２】ステップ２ｄにおいて、通信セッションがクライアントに対して構築され、検索されたアクセス制御規則が通信セッションに適用される。この方法においては、アクセス制御規則に従って、クライアントは、検索する資格が与えられていないディレクトリ情報を検索できないようにされる。図２は、ディレクトリクライアント４０とディレクトリサーバ４２との間の通信を示すが、この方法は、クライアントとサーバとに対して適用されることを意図する。たとえば、サーバはウェブサイトに行こうとするクライアントに対するアクセス制御規則を検索するよう動作することもある。

【００４３】図５は、この発明の例示的な実施例に従って実行される、一般的な動作シーケンスをフローチャートで示す。図５に示されるように、まずクライアントはクライアントを一意に識別する識別名（ＤＮ）を送信する（７０）。その後、サーバがその識別名ＤＮを受取る（７２）。

【００４４】ブロック７４に示されるように、サーバはクライアントＤＮを分析して、適用すべき適切なＡＣＬアクセス制御規則を判定する。ブロック７４において括弧内に「再帰的」と示すように、サーバは適用すべき適切なアクセス規則を判定するために、インターネットを通じて他のディレクトリサーバにアクセスすることもできる。アクセス制御規則に加えて、クライアントに関連する信頼の度合に関する情報もまた、インターネット上の種々のサーバからアクセスされ得る。サーバは、クライアントに適用されるべきアクセス制御規則および信頼規則を提供するために、インターネット上の他のディレクトリサーバに対して要求を行なうことでそれ自身がクライアントとなる。したがって、ウェブサイトのコンテキストにおいては、もしクライアントが自身の識別名ＤＮ（または代替的な識別子）をウェブサイトに対して送る場合、ウェブサイトは、それに関連するサーバにおける内部データベースにおいて、または他のウェブサイトにおいて、そのクライアントを識別する必要がある。ウェブサイトはその後、要求を発しているクライアントとの信頼関係を判定することができるまで、他のディレクトリサーバウェブサイトから識別情報を探すことが可能である。このように他のディレクトリサーバから検索された情報によって、要求を発しているクライアントに関連する信頼の度合を判定することが可能となる。

【００４５】ブロック７４の処理においてクライアントが検証されると、ブロック７６において示されるように、ＡＣＬ情報がディレクトリサーバに返されて、データ接続に適用される。アクセス制御規則および信頼に関連する情報は、データ接続に適用されて、データ接続中にアクセス制御規則および／または信頼情報に従って許可レベルを越えない範囲で、動作が確実に行なわれるようにする。

【００４６】この方法に従えば、たとえば、Ｖｉｓａが発行して、関係者が所持するデジタル証明書を、ウェブサイトに送信することが可能となり、電子取引が行なわれて、商品の購入が実現する。この取引は、たとえば、Ｖｉｓａのディレクトリサーバを通じてチェックされ得るクライアントの信用付けに従って行なわれ得る。Ｖｉｓａディレクトリサーバは、たとえば、ウェブサイトにおいて情報を要求している関係者および個別のクライアント等の、特定のコンテキストに応じて、送信すべき信用付けの性質を判定することが可能である。このプロセス中、ウェブサイトもまた同様に、Ｖｉｓａディレクトリサーバに対してそのデジタル証明書を送信して、Ｖｉｓａディレクトリサーバがそのウェブサイトがたとえば最近になって倒産した会社であるか、または、大きな度合の信用を与えられるべき別の銀行かを判定することができるようにする。このようにして、この発明は、取引パラメータが特定の通信または商取引コンテキストにおいて十分に展開できるようにする。

【００４７】図５のブロック７８に従えば、適切なアクセス制御リスト規則および／または信頼情報が得られると、それらの情報はデータ接続に適用される。要求されたデータは図５に示すように、クライアントに送り返されるが、アクセス制御規則または信頼レベル情報は通信されることはない。このプロセスは、後続の異なる通信セッションに関連して繰返され得る。

【００４８】図６および図７は、例示的な識別検証分析に関連する動作のシーケンスを示すフローチャートである。ディレクトリサーバ検証分析コンポーネントに入力されるデータは、たとえば図４に示されるようなデジタル証明書を含み得るクライアントの身元と、通信の性質および／または種類を説明するコンテキストディスクリプタである通信コンテキスト情報と、サーバのデジタル証明書であるサーバの身元とを含む。図６および図７に示されるディレクトリサーバ検証分析のフローチャートは、図２に示されるディレクトリサーバ４２内に実現されるソフトウェアによって実行される。

【００４９】図８は、例示的な検証ディスクリプタオブジェクトを示し、図９は、図６および図７に示される検証分析において利用されるコンテキストディスクリプタデータ構造の一例を示す。まず検証ディスクリプタに関して、図８に示されるデータ構造／オブジェクトは、クライアントを識別するデジタル証明書と、サーバを識別

するデジタル証明書と、コンテキストディスクリプタとを含む。コンテキストディスクリプタがヌルの場合、コンテキストはデフォルトとして、ディレクトリサーバプロトコルのコンテキストとなる。したがって、コンテキストディスクリプタが存在しない場合には、コンテキストはクライアントと、そのクライアントと通信するディレクトリサーバとの間の通信セッションであると推定される。これに代えて、もしウェブクライアントがウェブサーバと通信しておりウェブサーバが検証分析を行なう場合には、コンテキストディスクリプタはウェブクライアントと通信するウェブサーバを示すよう設定される。サーバの身元がヌルの場合には、サーバはデフォルトとしてディレクトリサーバ自身となる。ウェブクライアントとウェブサーバとの間に通信がなされる場合には、ウェブサーバはそのウェブの身元をそのデジタル証明書を介して入力する。

【００５０】図９に示すように、例示のコンテキストディスクリプタは、バージョン番号フィールドと、協定世界時を示す時間フィールドとを含む。「プロトコル」フィールドは、特定の通信コンテキストに応じて変化する。たとえば、もしウェブサーバがウェブクライアントと通信する場合には、プロトコルはウェブプロトコル「ｈｔｔｐ」であり得る。Ｅメールのクライアントがメールのサーバと通信している場合には、プロトコルは「ＳＭＴＰ」プロトコルであり得る。さらに、プロトコルによって規定されるいかなるパラメータも、コンテキストディスクリプタ内に列挙され得る。

【００５１】再び図６を参照して、ブロック８０において、ディレクトリサーバはデジタル証明書の発行者の公開鍵がディレクトリサーバに対して入手可能であるかをチェックする。たとえば、もしＶｉｓａが要求を発する関係者に対してデジタル証明書を発行した場合、たとえば、ウェブサイトにおいてチェックが行なわれて、そのウェブサイトがＶｉｓａを識別可能であるか、および、Ｖｉｓａの公開鍵へのアクセスを有するかどうかが判定される。もし証明書の発行者が既知である場合には、その証明書の発行者のデジタル署名を検証することが可能である。

【００５２】ブロック８０における分析に基づいて、証明書の発行者が既知かどうかに関する判定が行なわれる（８２）。もしその証明書の発行者が知られていなければ、ディレクトリはディレクトリクライアントとして動作して、既知の証明書発行者を発見しようと試みる。

【００５３】ディレクトリサーバが既知の証明書発行者を発見するためにディレクトリクライアントとして動作した後に、図７のブロック８４において、既知の証明書発行者が見つかったかどうかを判定するチェックが行なわれる。もし見つかれば、ルーチンは分岐してブロック８０に戻り、続行される。既知の証明書発行者が見つからなければ、アクセスは拒否される。

【００５４】ブロック８０における分析に関連して利用される例示的なデータ構造またはオブジェクトを図１０に示す。図１０に示されるように、証明書発行者の名称は、検証ディスクリプタのクライアントの身元および発行者の身元情報を使用することによって特定される。図１０に示すように、検証プロセスは、発行者の公開鍵および検証アルゴリズム識別子情報を利用する。もし図１０に示すデータ構造がヌルすなわちブランクの「発行者公開鍵」フィールドを有する場合、知られていない証明書発行者に対する解決策は、以下のいずれかを含む。すなわち、別のディレクトリサービスに対するディレクトリサービスクライアントとして動作して、ローカルキャッシュ内に別のディレクトリからの情報を格納する、または、アクセス制御規則がサーチされるまで、解決を据え置くことによって、知られていない署名を許可する、のいずれかである。知られていない署名の利用を許可することによって、システムは、それが適切であるかどうかを判定するアクセス制御規則に信頼をおきながらも、知られていない署名を受入れることが可能となる。たとえば、ウェブサイトによっては、証明書の発行者が誰であるかを問題にしないこともあり、実際に、アクセスされることを促すウェブサイトもある。このような状況下では、アクセス可能な制御リスト規則は、知られていない証明書発行者が含まれるコンテキストを特定する、特定の制約を含み得る。

【００５５】再び図６を参照して、もし証明書の発行者の公開鍵が入手可能であれば、ディレクトリサービスはブロック８６において、発行者の証明書上のデジタル署名が内部に記憶された証明書の発行者の公開鍵と合致するよう、デジタル署名を検証する。

【００５６】図１１は、図６のブロック８６における検証動作を実行するのに必要とされる、オブジェクトまたはデータ構造の一例を示す。図１１に示すように、図４に関連して先に説明したデジタル証明書内に実現される、署名されたシーケンスからなるクライアントの身元が使用される。アルゴリズム識別子を含む、示される情報を含む、発行者の公開鍵もまた使用される。したがって、デジタル証明書によって規定された署名されたシーケンスであるクライアントの身元により、その署名が発行者の公開鍵で検証できる。

【００５７】次に、図６のブロック８８において、その署名が良いかどうかを判定するためのチェックが行なわれる。もしその署名が悪いものであれば、図７に示すように、アクセスは拒否されるかまたは、先に説明したように、その問題を解決するための判定が、アクセス制御規則がチェックされるまで据え置かれる。

【００５８】ブロック８８におけるチェックによって署名が良いと示された場合には、ブロック９０に示すように、ディレクトリサービスが、内部に記憶された証明書の状態をチェックすることによって、その証明書が現在

もなお有効であることを検証する。場合により、内部に記憶された証明書取消しリストに対してチェックが行なわれることもある。

【００５９】図１２は、図６のブロック９０に示される検証を行なうのに使用され得る、例示的なオブジェクトまたはデータ構造を示す。図１２に示すように、クライアント身元情報は、先に説明したデジタル証明書を含む。証明書取消しリストとは、先に取消された証明書のリストであって、属性－シンタックス証明書リストで、属性として表わされ得る。このリストは、図１２に示されるような証明書の署名されたシーケンスの形をとり得る。署名されたシーケンスは、証明書のシリアル番号と取消しの日付とを含む。この証明書取消しリストは、統御ディレクトリサービスエンティティによって作成され得る。もしクライアントを識別する証明書シリアル番号がディレクトリサービスに保持される証明書取消しリスト内に記憶されていて証明書が取消される場合には、証明書取消しリストは適正に許可された者によってのみ修正され得る。取消しリストを作成および改訂できるのは、ディレクトリサービスに接続する、通常のクライアントよりもより拡張された権利を有する権限のみである。そのような権限は、証明書取消しリストのようなデータ構造に書込みができる権限を含む。このような接続は、通常ディレクトリサービスの管理者のデジタル証明書を用いてのみなされるものである。ディレクトリサービスは、完全な証明書取消しリストを保持する必要はない。なぜなら、それは、ディレクトリサービス内に記憶された生のデータから構築することが可能なためである。したがって、特定の証明書が有効ではないことを示す情報を、ディレクトリサービス内に記憶してもよい。ディレクトリサービス内に記憶された生のデータは、証明書ごとに、有効性を調べる目的でルックアップが可能である。証明書取消しリストは、ローカルキャッシュから、もしくは別のディレクトリサービスから検索されるか、または、ＡＣＬ規則がチェックされるまで据え置くことが可能である。

【００６０】再び図６を参照して、ブロック９０における処理に基づいて、有効な証明書があるかどうかを判定するチェックが行なわれる（９２）。ブロック９２におけるチェックによって判定された結果、もし有効な証明書がない場合には、接続は拒否されるか、または、先に記載したように据え置かれる。

【００６１】もし有効な証明書がある場合には、ブロック９４の処理に従って、ディレクトリはクライアントの証明書、サーバの証明書および通信コンテキストを比較対照して、クライアント接続に適用すべきアクセス制御規則を内部に記憶されたアクセス制御規則から検索する。

【００６２】図１３は、図６のブロック９４の処理においてアクセス制御規則を検索するために使用され得る、例示のオブジェクトまたはデータ構造を開示する。アクセス制御規則の一例は図１４に示す。アクセス制御規則の組は、ディレクトリサービスデータベース内に規定される。種々のディレクトリサーバを連結することによって、適用すべきアクセス制御規則を完璧に判定するために、他のディレクトリサーバ内に記憶されているアクセス制御規則を利用できるようにおよび要求できるようにすることが可能である。ディレクトリサーバは、予め取り決められた契約上の信頼関係に基づいて連結することが可能である。たとえば、Ｖｉｓａカードに関する信頼関係においては、Ｖｉｓａが所与の商店主およびカード保持者を信頼し、その商店主がＶｉｓａカード保持者を信頼しなくてはならない。ＡＣＬ規則は、コンテキストとクライアントの証明書とサーバの証明書とを使用することによって、サーバ自体によってアクセスされる。ＡＣＬ規則は、クライアントの身元、コンテキストディスクリプタ（これはたとえば、Ｅメールまたはウェブサイトに関連する取引が含まれるかどうかを示す）、およびサーバの身元とに基づいて、サーバの内部データベースから検索される。

【００６３】図１４に示すように、ＡＣＬ規則は、たとえば規則がウェブページに適用されることを示す、「ｔｏ　ｗｈａｔ」フィールドを含む、デジタルシーケンスである。ＡＣＬ規則はまた、「ｔｏ　ｗｈａｔ」フィールドに関連する、たとえばウェブページアドレスもしくはクレジットカード番号、カードの性質および／またはカード保持者の名称等を含むパラメータもまた含み得る。「ｂｙ　ｗｈａｔ」フィールドもまた含まれ得るが、これは通常、クライアントＩＤによって識別され得るクライアントの証明書を含む。たとえば、デジタル証明書であり得る「ｂｙ　ｗｈａｔ」パラメータが含まれる。「ａｃｃｅｓｓ」フィールドもまた含まれるが、これは、許可され得るディレクトリのアクセスモードを規定する整数からなる。例示の目的で、アクセス整数０～４は、それぞれ、サーチ、比較、読出、書込、または空を示す。アクセス制御規則は、バージョン番号もまた含み得る。

【００６４】証明書発行者の署名または証明書取消しリストをチェックする動作が図６のブロック９４の処理まで据え置かれる場合には、これらの事象は図１３に示されるコンテキストフィールドの一部として渡される。さらに、証明書取消しリストは、据え置かれた場合には、アクセス制御規則リストの一部であり得る。また、信用レベルがアクセス制御リスト規則内で規定され得ることにも注目されたい。アクセス制御規則は、ローカルキャッシュメモリから、または、別のディレクトリサービスから検索することができる。アクセス制御規則がいかなるときにローカルで保持されねばならないか、また、どのようなときに別のディレクトリサービスから検索することが可能であるかについては、どのような制限を課す

ことも可能である。

【００６５】再び図６を参照して、アクセス制御規則はデータ接続に適用されて、それにより、クライアントのみが正しくかつ意図されたデータを受信できるようにされる。したがって、検証コンポーネントは、クライアントに適用されるべきアクセス規則を、サーバに対して返すのである。

【００６６】以上に、この発明を、現時点で考えられる最も実用的かつ好ましい実施例に関連して説明したが、この発明が開示された実施例に限定されるものではなく、逆に、前掲の請求項の範囲および精神内に含まれる種々の修正および等価構成物をも網羅するものであると理解されたい。

【図面の簡単な説明】

【図１】この発明が中で利用され得る、例示的な通信システムのブロック図である。

【図２】ディレクトリクライアントとサーバとの間で通信される例示的なデータを示すデータフロー図である。

【図３】クライアントがいかにして安全な通信プロトコルで特定され得るかを示す、データフロー図である。

【図４】図３に関連して使用され得る、デジタル証明書の一例を示す図である。

【図５】例示の実施例に従って行なわれる動作の一般的なシーケンスを示すフロー図である。

【図６】識別検証プロセスに含まれる動作のシーケンスの一例を示すフロー図である。

＊【図７】識別検証プロセスに含まれる動作のシーケンスの残りの部分を示すフロー図である。

【図８】検証ディスクリプタオブジェクト／データ構造の例を示す図である。

【図９】コンテキストディスクリプタオブジェクト／データ構造の例を示す図である。

【図１０】図６のブロック８０における検証分析に関連して利用される、データ構造／オブジェクトの例を示す図である。

【図１１】図６のブロック８６における検証分析を実行するのに使用される、オブジェクト／データ構造の例を示す図である。

【図１２】図６のブロック９０における検証分析を実行するのに使用されるオブジェクトの例を示す図である。

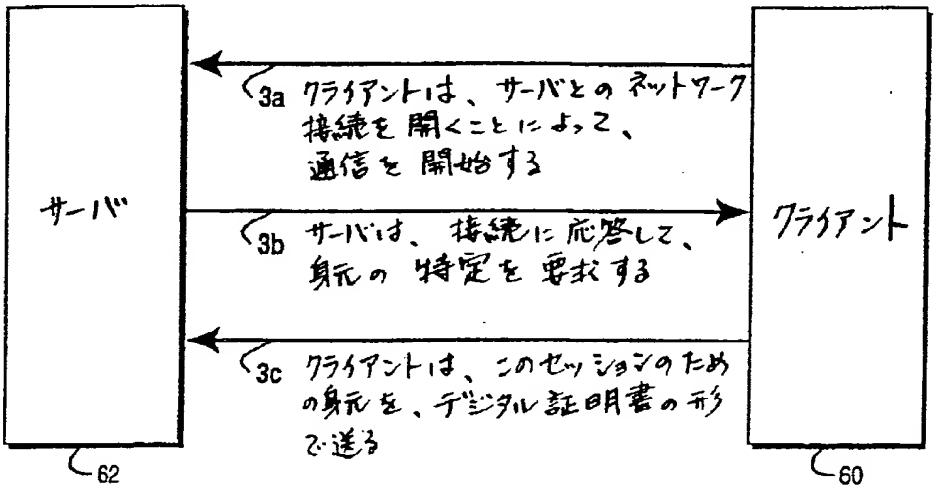
【図１３】アクセス制御リスト規則を検索するのに使用される、オブジェクト／データ構造の例を示す図である。

【図１４】アクセスリスト制御規則オブジェクト／データ構造を示す図である。

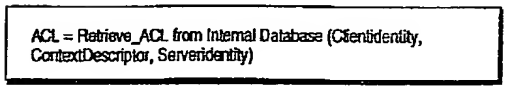
【符号の説明】

４０　ディレクトリクライアント
４２　サーバ
４４　ディレクトリサーバ
４６　通信プロトコルコンポーネント
４８　ディレクトリアクセスコンポーネント
５０　内部ディレクトリデータベース

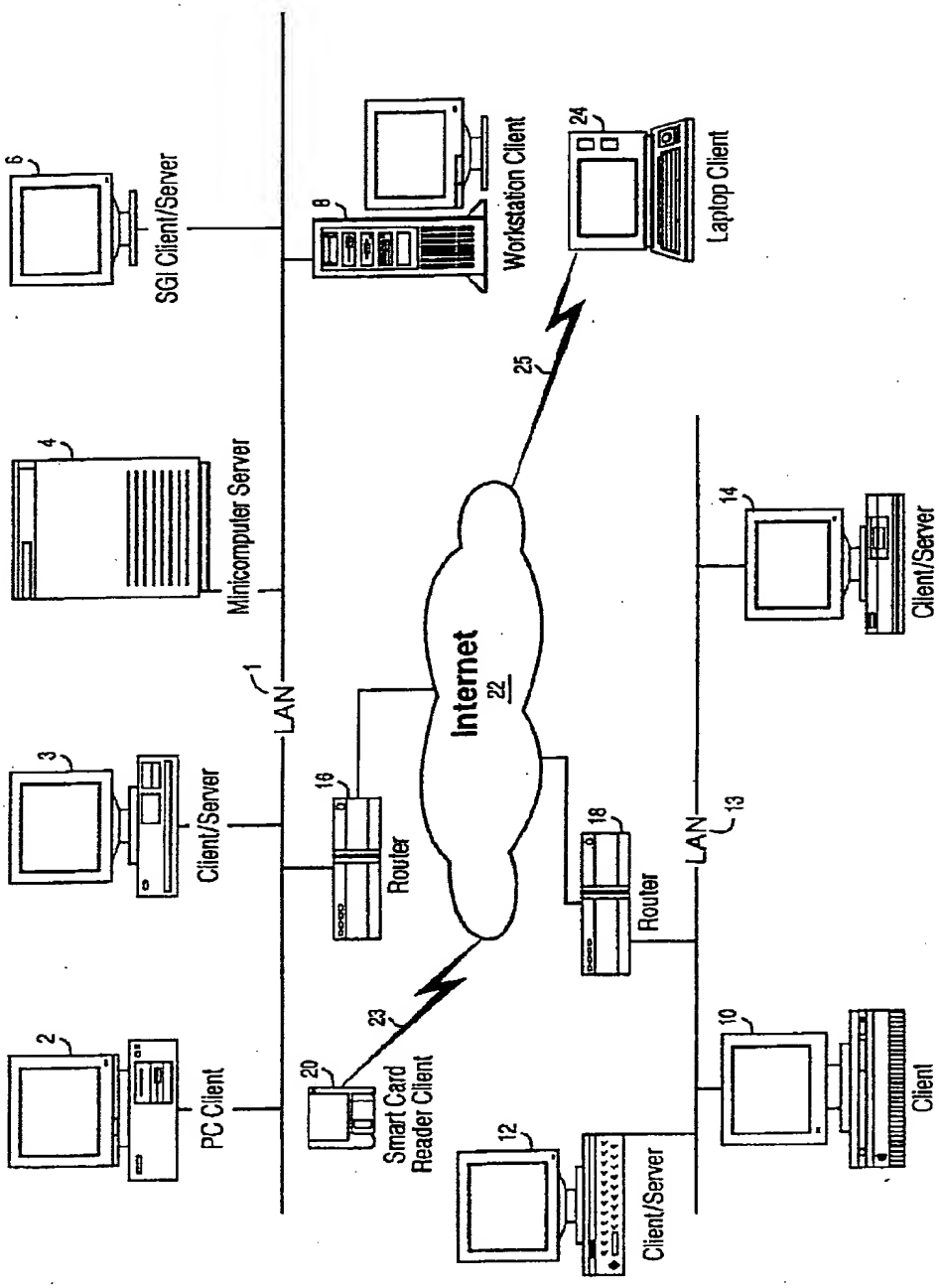
【図３】



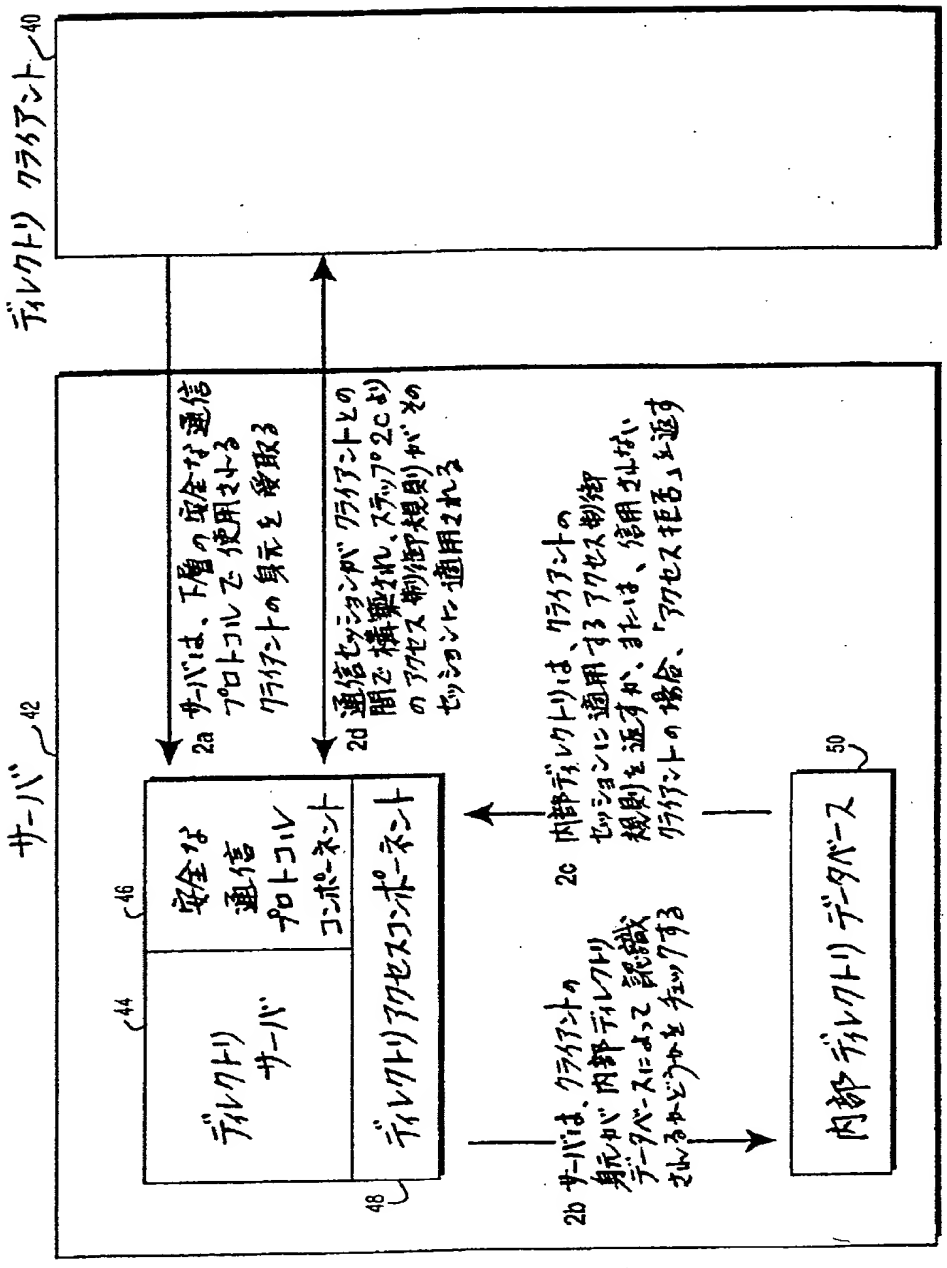
【図１３】



【図１】


SGI Client/Server
6
Workstation Client
8
Laptop Client
24
25
Minicomputer Server
4
LAN
1
Internet
22
Client/Server
14
Client/Server
3
Router
16
Router
18
LAN
13
PC Client
2
23
Smart Card
Reader Client
20
Client/Server
12
Client
10

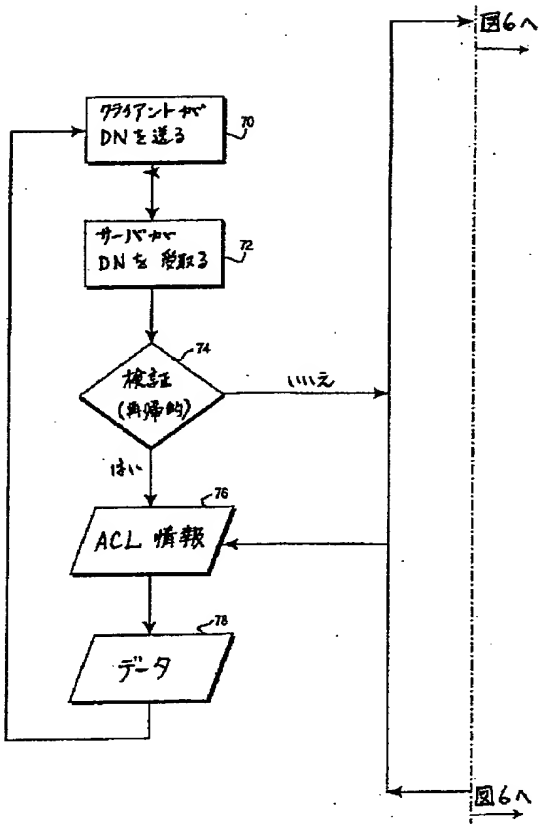
【図２】


ディレクトリ クライアント 40
サーバ 42
2a サーバは、下層の安全な通信プロトコルで使用されるクライアントの身元を受取る
2d 通信セッションがクライアントとの間で構築され、ステップ2cよりのアクセス制御規則がそのセッションに適用される
ディレクトリ サーバ 44
安全な通信プロトコルコンポーネント 46
ディレクトリアクセスコンポーネント 48
2b サーバは、クライアントの身元から内部ディレクトリデータベースによって認識されるかどうかをチェックする
2c 内部ディレクトリは、クライアントのセッションに適用する3アクセス制御規則を返すが、または、信用されないクライアントの場合、「アクセス拒否」を返す
内部ディレクトリデータベース 50

【図４】

```
Certificate        ::= SIGNED SEQUENCE{                          64
        version                 [0]Version DEFAULT 1988,
        serialNumber            SerialNumber,
        signature               Algorithmidentifier
        issuer                  Name
        validity                Validity,
        subject                 Name,
        subjectPublicKeyInfo    SubjectPublicKeyInfo}
Version            ::= INTEGER { 1988(0)}
SerialNumber       ::= INTEGER
Validity           ::= SEQUENCE{
        notBefore               UTCTime,
        notAfter                UTCTime}
SubjectPublicKeyInfo    ::= SEQUENCE{
        algorithm               Algorithmidentifier
        subjectKey              BIT STRING}
Algorithmidentifier ::= SEQUENCE{
        algorithm               OBJECT IDENTIFIER
        parameters              ANY DEFINED BY algorithm
                                OPTIONAL}
```

【図５】



【図８】

```
Verification_Descriptor     ::= SEQUENCE{
        Clientidentity          Certificate,
        ContextDescriptor       Context,
        Server identity         Certificate }
```

【図９】

```
Context   ::= SEQUENCE{
        version                 [0]Version DEFAULT 1996,
        time                    UTCTime,
        protocol                OBJECT IDENTIFIER
        parameters              ANY DEFINED BY protocol
                                OPTIONAL}
Version        ::= INTEGER { 1996(0) }
```

【図１０】

```
IssuerName = Verification_Descriptor->Clientidentity->Issuer
IssuerPublicKey =   ::= SEQUENCE{
        algorithm               Algorithmidentifier
        Key                     BIT STRING}
Algorithmidentifier    ::= SEQUENCE{
        algorithm               OBJECT IDENTIFIER
        parameters              ANY DEFINED BY algorithm
                                OPTIONAL}
```

【図１１】

```
Clientidentity ::= SIGNED SEQUENCE{
        ...
        }
IssuerPublicKey =   ::= SEQUENCE{
        algorithm               Algorithmidentifier
        Key                     BIT STRING}
Algorithmidentifier    ::= SEQUENCE{
        algorithm               OBJECT IDENTIFIER
        parameters              ANY DEFINED BY algorithm
                                OPTIONAL}
```

【図１２】

```
Clientidentity  ::= Certificate
CertificateRevocationList     ::= ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX CertificateList
AuthorityRevocationList       ::= ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX CertificateList
CertificateList               ::= SIGNED SEQUENCE{
        signature Algorithmidentifier,
        Issuer Name,
        lastUpdate UTCTime,
        revokedCertificates
                SIGNED SEQUENCE OF SEQUENCE{
                signature Algorithmidentifier,
                Issuer Name, CertificateSerialNumber subject,
                revocationDate UTCTime}
        OPTIONAL}
```

【図６】

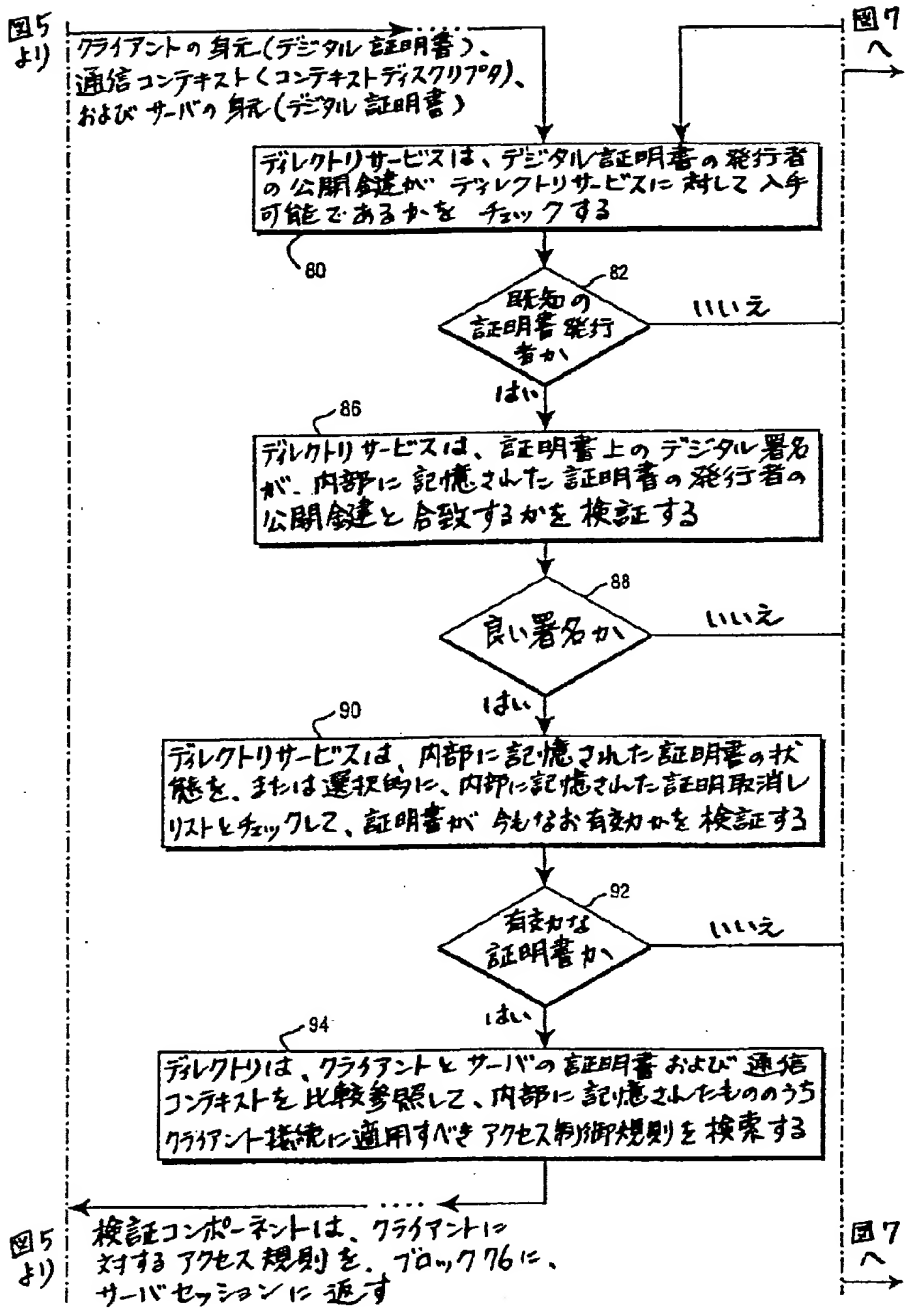


図5より
クライアントの身元(デジタル証明書)、通信コンテキスト(コンテキストディスクリプタ)、およびサーバの身元(デジタル証明書)
ディレクトリサービスは、デジタル証明書の発行者の公開鍵がディレクトリサービスに対して入手可能であるかをチェックする
80
既知の証明書発行者か
82
いいえ
はい
ディレクトリサービスは、証明書上のデジタル署名が、内部に記憶された証明書の発行者の公開鍵と合致するかを検証する
86
良い署名か
88
いいえ
はい
ディレクトリサービスは、内部に記憶された証明書の状態を、または選択的に、内部に記憶された証明取消しリストとチェックして、証明書が今もなお有効かを検証する
90
有効な証明書か
92
いいえ
はい
ディレクトリは、クライアントとサーバの証明書および通信コンテキストを比較参照して、内部に記憶されたもののうちクライアント接続に適用すべきアクセス制御規則を検索する
94
検証コンポーネントは、クライアントに対するアクセス規則を、ブロック76に、サーバセッションに返す
図5より
図7へ
図7へ

【図７】

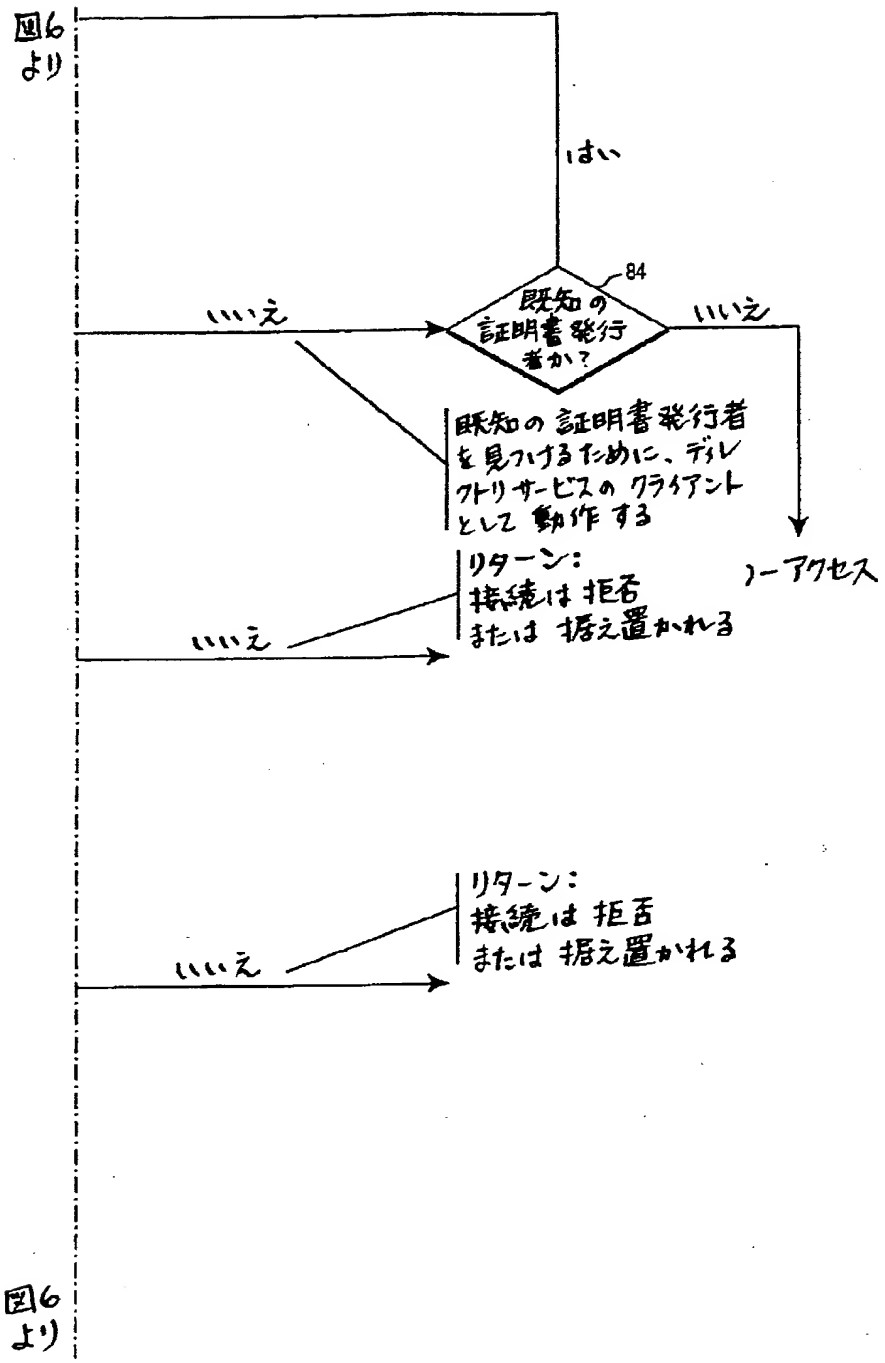
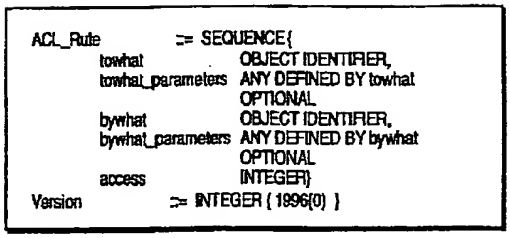


図6より
はい
84
既知の証明書発行者か？
いいえ
いいえ
既知の証明書発行者を見つけるために、ディレクトリサービスのクライアントとして動作する
リターン：接続は拒否または据え置かれる
)ーアクセス
いいえ
リターン：接続は拒否または据え置かれる
いいえ
図6より

【図１４】



フロントページの続き

(72)発明者　パトリック・リチャード
カナダ、ブイ・７・ワイ　１・シィ・６
ブリティッシュ・コロンビア州、バンクーバー、パシフィック・センタ、ピィ・オゥ・ボックス・10145、ダブリュ・ジョージア・ストリート、701、スウィート・1001

(72)発明者　アンドリュー・スィンガー
カナダ、ブイ・７・ワイ　１・シィ・６
ブリティッシュ・コロンビア州、バンクーバー、パシフィック・センタ、ピィ・オゥ・ボックス・10145、ダブリュ・ジョージア・ストリート、701、スウィート・1001

(72)発明者　ブルース・ナイブ
カナダ、ブイ・７・ワイ　１・シィ・６
ブリティッシュ・コロンビア州、バンクーバー、パシフィック・センタ、ピィ・オゥ・ボックス・10145、ダブリュ・ジョージア・ストリート、701、スウィート・1001

(72)発明者　ブルース・ウッドワード
カナダ、ブイ・７・ワイ　１・シィ・６
ブリティッシュ・コロンビア州、バンクーバー、パシフィック・センタ、ピィ・オゥ・ボックス・10145、ダブリュ・ジョージア・ストリート、701、スウィート・1001